A New Framework using UID based Digital Signature Certification System

A
Synopsis
Submitted by
(Sunil Digambarrao Potekar)

Under the guidance of
Dr. Sudhir Jagtap

in fulfillment for the award of the degree
Of
DOCTOR OF PHILOSOPHY

Swami Ramanand Teerth Marathawada University
Nanded

INDEX

Sr.No.	Content	Page Number
1	Abstract of proposed work plan / Problem	3
2	Introduction	4
3	Review of literature and Development in the subject	6
4	Objectives of Research / Proposed Hypothesis	12
5	Methodology to be adopted	13
6	Importance of study / society application	14
7	Proposed work plan	15
8	References	16

Abstract of proposed work plan / Problem

Information and Communication Technology (ICT) has become core medium for implementation of various schemes and policies across the world. Government of India has taken various initiatives for implication of ICT in Governance in recent years. The implication of online systems for various departments has been started in the recent years. For the security and integrity of data is traditionally achieved by login and password. The login/password authenticity is further transformed to biometric thumb impression validation and further enhanced by Digital Signature Certificates (DSCs).

The main objective of the present research is to study the Study of Digital Signature Certificates (DSCs) given by licensed Certifying Authorities (CAs) in India with predefined parameters. The study of various technical aspects will be further extended to suggest a simplified solution for DSCs generation and usage. The process will be redesigned within the frame of terms and conditional as prescribed by CCA.

A simplified algorithm may be suggested that will be based on UID. The usage methodology of the proposed algorithm will be explained for its usage method. The simplified algorithm may be verified against the difficulties found in the hypothesis. Other Unique identification schemes may be used for the simplification of the issuance and usage.

Introduction

Information and Communication Technology (ICT) has become core medium for implementation of various schemes and policies by Government across the world. Government of India has taken various initiatives for implication of ICT in Governance in recent years.

National Informatics Center (NIC) is established in 1976. NIC has developed number of e-Governance applicationsand implemented it to up to the grassroots level. National Informatics Center Network (NICNET) has institutional linkages with all the Ministries /Departments of the Central Government, 36 State Governments/ Union Territories, and about 688 District administrations of India. The services provided by NIC includes, Anti Virus, Business Intelligence, Cloud Services, CollabLand Computer Aided Design, Domain Registration, e-Governance Standards, ICT Training, Integrated Network Operations, Messaging, National Data Centres (NDCs), NKN (National Knowledge Network), Open Technology Group, Remote Sensing and Geographical Information System (GIS), Satellite Communication (SATCOM), Utility Mapping, Video Conferencing, Web Services and Webcast.

Department of Electronics and Information Technology (DeitY) is operational under Ministry of Information and Communication Technology (MICT) in Government of India. The DeitY has formulated a National e-Governance Plan (NeGP) for integrating various eGovernance efforts by various State Governments across the country in the year 2006. (Revised in year 2011). NeGP has 31 Mission Mode Projects and 8 components covering almost all sectors of Government-to-Citizen (G2C), Government-to-Government (G2G) activities.

National Information Technology Policy is formulated and implemented in year 2012. focuses on application of technology-enabled approaches to overcome monumental developmental challenges in education, health, skill development, financial inclusion, employment generation, governance etc. to greatly enhance efficiency.

The Digital India programme is a Dream Project of the Government of India anpunced in the year 2015. The main vision of Digital India to transform India into a digitally empowered society and knowledge economy.

The main goal of all these efforts is to bring transparency, accuracy and speed in government process. Implication of ICT by reengineering the Government Process has

proved effective in most of the projects implemented at various levels of Government officials.

Adoption new technology has brought the technical threats in the process and need arrived where the issues were handled in jurisdiction of Indian Judiciary System. Indian IT Act was formulated and imposed in the year 2000 and further amended in year 2002. The implication of online systems for various departments has been started in the recent years. The security and integrity of government and citizen data are the major concerns in the implementation. The authenticity of users is the major concern in validating the genuineness of the users accessing the data at various levels in the process. Despite of highest security protocols adopted at the Data Centers users level security is very important aspect. User authentication is traditionally achieved by login and password.

The login/password authenticity is further transformed to biometric thumb impression validation and further enhanced by Digital Signature Certificates (DSCs) given to the authorized users of the system. As per Section 18 of The Information Technology Act, 2000 provides the required legal sanctity to the digital signatures based on asymmetric cryptosystems. The IT Act provides for the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities. The Certifying Authorities (CAs) issue digital signature certificates for electronic authentication of users.

Various eGovernance applications are designed and implemented where the DSC feature is integrated to achieve the higher security level. The number of DSC based applications are increasing day-by-day. More and more number of users are procuring DSCs.

Review of literature and Development in the subject (Previous work done in the relevant area)

The present topic is concerned with present trends of eGovernance in India. There are TWO types of literature is reviewed for completing the study.

1. Government policy documents and Acts
2. Research works in the relevant area.

The major source of literature is government websites, IEE Explore – Digital Library (the researcher is having the authentic access to the IEE Digital Library through NICNET. Academic books for technical reference will be made available from Study Centre .

The important documents required for present study are as follows,

1. National Policy on Information Technology, 2012 (NPIT 2012) available at http://deity.gov.in/sites/upload_files/dit/files/National_20IT_20Policyt%20_20.pdf It says that one of the main objective is "To strengthen the Regulatory and Security Framework for ensuring a Secure and legally compliant Cyberspace ecosystem." Under "Security of Cyber Space", it elaborate further as "9.1 To undertake policy, promotion and enabling actions for compliance to international security best practices and conformity assessment (product, process, technology & people) and incentives for compliance. 9.2 To promote indigenous development of suitable security techniques & technology through frontier technology research, solution oriented research, proof of concept, pilot development etc. and deployment of secure IT products/processes 9.3 To create a culture of cyber security for responsible user behavior & actions including building capacities and awareness campaigns. 9.4 To create, establish and operate an 'Information Security Assurance Framework.'"
2. Strategies for E-Governance in India were explained at http://indiaegovernance.blogspot.in/2008/04/strategies-for-e-governance-in-india.html Scope, Objectives, Ascepts and Stages of eGOvernance were discussed in a blogpost by Shri. Abhijeet A. Joshi.
3. http://negd.gov.in/ is official website of National eGovernance Division (NeGD) that elaborate the Vision Areas of Digital India Program.
4. "e-Governance : "Initiatives in India" is full text at http://arc.gov.in that elaborate the relevance information for present study as follows,

   "G2G services and linkages: The architecture of MCA 21 has been designed to meet future challenges and scalability. It is capable of sharing information with other Government Departments/ Ministries/ Regulators in the Corporate Sector and introduction

of joined-up services in due course. Presently, free access to company documents having been allowed to the following organisations:

i. Reserve Bank of India;

ii. Financial Intelligence Unit (FIU-IND);

iii. Department of Economic Affairs;

iv. Intelligence Bureau; and

v. Central Statistical Organisation.

Access has been permitted to designated officers in these offices through a secure DSC based login. Once the other Departments implement their e-Governance programmes, and the NSDG develops the national Gateway, the MCA 21 system can be linked with more organizations

5. The national portal of India, https://india.gov.in/ , official website of DeiyT, http://deity.gov.in/ and Official website of National Informatics Centre http://www.nic.in/ gives the information of other policies of Government. “In order to promote e-Governance in a holistic manner, various policy initiatives and projects have been undertaken to develop core and support infrastructure. The major core infrastructure components are State Data Centres (SDCs), State Wide Area Networks (S.W.A.N), Common Services Centres (CSCs) and middleware gateways i.e National e-Governance Service Delivery Gateway (NSDG), State e-Governance Service Delivery Gateway (SSDG), and Mobile e-Governance Service Delivery Gateway (MSDG). The important support components include Core policies and guidelines on Security, HR, Citizen Engagement, Social Media as well as Standards related to Metadata, Interoperability, Enterprise Architecture, Information Security etc.” explained at DeitY official website. The full text of documents of Notification under IT(Amendment) Act, 2008, IT (Amendment) Act 2008(2349 KB) PDF file that opens in a new windowThis pdf file is non accessible through use of Assistive Technologies (i.e.screen-readers). For user information Document title is "The Gazette of India Part II" Dated February 5,2009. For More information contact DIT webmaster, IT Act 2000, Rules for the Information Technology Act 2000 and Report of the Expert Committee on Amendments to IT Act 2000 are available at http://deity.gov.in/content/information-technology-act
6. “The Controller of Certifying Authorities (CCA) has been appointed by the Central Government under section 17 of the Act for purposes of the IT Act. The Office of the CCA came into existence on November 1, 2000. It aims at promoting the growth of E-Commerce and E- Governance through the wide use of digital signatures” texted at official website of CCA, http://www.cca.gov.in/cca/ which also gives the full text of

"Interoperability Guidelines for Digital Signature Certificates issued under Information Technology Act".

7. "Certificate Profile Guidelines : One of the most important aspects of interoperability is the uniform interpretation of Digital Certificate fields and extensions. The Certificate Profile Guidelines specifies the format of the digital certificate and classifies each of the fields / extensions as following:

   Mandatory – These fields or extensions are mandated by the CCA and MUST be present in the certificates issued by the Certifying Authorities. Additionally the content of the fields MUST be as per the guidance provided in this document.

   Optional – The CA may use this field at its discretion. However, in case the field is being used, the applicable guidance or the compliance standards specified MUST be adhered to.

   Special Purpose – These fields may be used only in certain circumstances. In all such cases, additional guidance will be provided by the CCA

   Customizable – Customizable fields are non standard extensions notified by CCA which may have interpretations depending upon usage / application / industry.

   Prohibited – These fields or extensions are NOT to be included or used in Digital Certificates unless notified by CCA regarding the usage and format.", were listed at http://www.cca.gov.in/cca/sites/default/files/files/DigitalSignatureCertificateInteroperabilityGuidelinesR3.1.pdf. The specification also provides guidance on other important aspects of the field including the length, data type and mandated values. The certifying authorities must issue certificates in accordance with the guidance provided in this documents.
8. Along with the vision, mission, and description of various function of CCA, the requirements fulfilled by the RCAI are explained at http://www.cca.gov.in/cca/ . "The CCA has established the RCAI under section 18(b) of the IT Act to digitally sign the public keys of CAs in the country. The RCAI is operated as per the standards laid down under the Act" It further explains, "Authorized CCA personnel initiate and perform Root CA functions in accordance with the Certification Practice Statement of Root Certifying Authority of India. The term Root CA is used to refer to the total CA entity, including the software and its operations."
9. The most informative part of http://www.cca.gov.in/cca/ for the present study is the complete documentation of all licensed CAs in India. Safescrypt, http://www.safescript.com/ Institute for Development & Research in Banking Technology (IDRBT), http://www.idrbt.ac.in/ , National Informatics Centre (NIC), http://www.nic.in Tata Consultancy Services (TCS) http://www.tcs.com/ nCode Solutions

https://www.ncodesolutions.com/, eMudhra Limited http://www.e-mudhra.com/ and Center for Development of Advance Computing (CDAC) http://www.cdac.in/ are SEVEN Licensed CAs in India. The CCA's official website gives the full text of Certification Practice Statement (CPS) of all seven Licensed CAs. The CPS includes, Overview, Identification, Agencies and Applicability along with General Provisions like Obligations, Liabilities and Financial Responsibilities. The CPS further elaborates the Certificate Application, Certificate Issuance, Certificate Download and Acceptance Certificate Revocation List (CRL),System Security Audit Procedures, Archival and Retention period Key Changeover & Compromise and Disaster Recovery under Operational Requirements of usage of individual DSC. Physical, Procedural and Personal Security Controls are fully described by each CA is respective CPS. Finally every document explores the Technical Security Controls. Key Pair Generation and Installation, Private Key Protection, Computer/Systems Security Controls, Network Security Controls and Cryptographic Module Engineering Controls are the technical issues explained in CPS. The following tables show the basic fields for CA Certificates. Sample of CDAC CA is shown in the Table1.1 below

Version	Version 3
Serial number	Positive number of maximum Length 20 bytes and unique to each certificate issued by a issuer CA
Signature Algorithm	SHA256 with RSA Encryption (null parameters
Issuer DN	Subject DN of the issuing CA
Validity	Validity expressed in UTC Time for certificates valid through 2049
Subject DN	The X.500 distinguished name of the entity associated with the public key certified in the subject public key field of the certificate (Common Name (CN),House Identifier, Street Address, State / Province, Postal Code, Organisational Unit (OU),Organisation (O),Country (C))
Subject Public Key	rsaEncryption {1 2 840 113549 1 1 1}, 2048 RSA Key modulus, public exponent
Signature	Issuer CA's signature

Table 1.1 – CDAC Basic fields for CA Certificates

The details Algorithm Object Identifiers are also expressed is CPS. An example of "C-DAC CA supports the following algorithms" is as below.

a. RSA 2048 digital signature in accordance with PKCS#1
b. RSA 2048 key transfer in accordance with Internet RFC 1421 and 1423 and PKCS#1
c. SHA-2 in accordance with US FIPS PUB 180-1 and ANSI X9.30 (Part2)
d. Triple-DES in accordance with ANSI X9.52
e. Message Authentication Code (MAC) in accordance with US FIPS PUB 113, ANSI X9.9 and X9.19
f. DSA, ECDSA, AES, DES, IDEA, CAST-128

The second part of literature reviewed to support of the present study is about the research works carried across the world about the DSCs. Following are the primarily concerned technical research works carried out so far in the research area.

1. A research paper “A New Certificate-based Digital Signature Scheme” is presented in Fourth International Conference on Emerging Intelligent Data and Web Technologies (2013) by Jianglang Feng and Jindong Li. “we present a certificate-based signature scheme derived from bilinear pairings and prove its security in the random oracle model. The scheme is secure based on the traditional difficult problem defined in bilinear pairings. The efficiency is also presented to show the scheme is practical. Compared to earlier signatures with these properties, our scheme is efficient. Many other constructions could be derived by using this certificate-based signature in applications”
2. IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 10, NO. 7, JULY 2011, Generalized Digital Certificate for User Authentication and Key Establishment for Secure Communications by Lein Harn and Jian Ren, explains, “public-key digital certificate itself cannot be used as a security factor to authenticate user. In this paper, we propose the concept of generalized digital certificate (GDC) that can be used to provide user authentication and key agreement. A GDC contains user’s public information, such as the information of user’s digital driver’s license, the information of a digital birth certificate, etc. Based on this concept, we propose both discrete logarithm (DL)-based and integer factoring (IF)-based protocols that can achieve user authentication and secret key establishment.”
3. Chen-huang WU has published a research paper on “Self-Generated-Certificate Digital Signature” at Fourth International Conference on Genetic and Evolutionary Computing (2010). The study express the concept, “New paradigm called Self-Generated-Certificate Public Key Cryptography(SGC-PKC) that captures the DoD Attack.Moreover, they provided a generic construction of a self-generated certificate public key encryption scheme in the standard model but without a self-generated-certificate public key signature scheme. In this paper, to the best of our knowledge, we give the first precise definition and security notions for Self-Generated-Certificate Digital Signature and then the first concrete signature scheme which is provably secure under the CDH assumption.”
4. “COMPARISON AND EVALUATION OF DIGITAL SIGNATURE SCHEMES EMPLOYED IN NDN NETWORK” is another study by Al Imem Ali published in International Journal of Embedded systems and Applications(IJESA) Vol.5, No.2, June 2015. “RSA and ECDSA as digital signature algorithms have proven their efficiency against cyber-attacks, they are characterized by their speed to encrypt and decrypt data, in addition to their competence

at checking the data integrity." The main purpose is find optimal algorithm that avoids the system's overhead and offers the best time during the signature scheme.

5. "Proposal and evaluation of the digital certificate system with sumi-coating module for privacy protection" was proposed by TAKASHI SAKUMA and RYOICHI SASAKI at IEEE 36th International Conference on Computer Software and Applications Workshops (2012) "A trusted certification authority enables the authentication of communicators and/or signers using digital certificate published from the certificate authority. The digital certificate contains information such as names or addresses, etc., which can be used to identify the individual, although a common opinion is it is a privacy problem to disclose such information. In this paper, therefore, we propose a digital certificate system using the revised sumi-coated signature to solve the privacy as well as the security problems."
6. "Cryptanalysis and Improvement of Several Digital Signature Schemes" is another research study by Huaqun Wang and Shuping Zhao, presented at Second International Conference on Networks Security, Wireless Communications and Trusted Computing (2010). They have compared the two DSCs proposed by Zhang and Ming in the year 2007 and conluded that, "We found that the two signature schemes couldn't resist the public key substitution attack or the malicious KGC (Key Generation Center) attacks. In order to avoid these flaws, we improve the last two digital signature schemes. The improved schemes are provably secure"

Objectives of Research / Proposed Hypothesis

The use of DSC based eGovernance applications is spreading in various departments. There are number of users involved in the administrative process at various levels, from Central Ministry level officials to Block level officials. There are limited CAs, as approved by CCA, are providing DSCs across the country. The present research work is based on the hypothesis that is some difficulties in usage of DSC by the non technical officials.

Hypothesis: The usage of DSC is difficult process for officials.

The main objective of the present research is to study the Study of Digital Signature Certificates (DSCs) given by licensed Certifying Authorities (CAs) in India. The study of various Signature Algorithms used by SEVEN licensed CAs. Following are the parameters to be studied for each CA,

1. Certificate Application, Certificate Issuance,
2. Certificate Download and Acceptance
3. Certificate Revocation List (CRL)
4. System Security Audit Procedures Archival
5. Retention period Key Changeover & Compromise
6. Disaster Recovery under Operational Requirements
7. Physical, Procedural and Personal Security Controls
8. Technical Security Controls.
9. Key Pair Generation and Installation
10. Private Key Protection
11. Computer/Systems/Network Security Controls
12. Cryptographic Module Engineering Controls

Study the above features of all, Seven CAs, i.e. Safescrypt, Institute for Development & Research in Banking Technology (IDRBT), National Informatics Centre (NIC), Tata Consultancy Services (TCS), nCode Solutions, eMudhra Limited and Center for Development of Advance Computing (CDAC). The study of various technical aspects of all the seven CAs will be further extended to suggest a simplified solution for DSCs generation and usage.

Methodology to be adopted

The present work is technical study of DSCs provided by licensed CAs in India. This involves classification of parameters based on technical features and usage related features of these DSCs. Following are the seven licensed CAs as on today (May 2016),

1. Safescrypt
2. Institute for Development & Research in Banking Technology (IDRBT)
3. National Informatics Centre (NIC)
4. Tata Consultancy Services (TCS)
5. nCode Solutions
6. eMudhra Limited
7. Center for Development of Advance Computing (CDAC).

For, present research work the CPS of these CAs will be compared. The technical details are studied on the basis of predefined parameters. The technical discussions with the CAs may be planned to clarify technical doubts.

The DSC issuance process, its download and acceptance by the user will studied along with its usage procedure will be studied on the basis of hypothesis. The process will be redesigned within the frame of terms and conditional as prescribed by CCA.

A simplified algorithm may be suggested with explanation of its usage method. The simplified algorithm may be verified against the difficulties found in the hypothesis. The implication of UID may be suggested for DSC issuance and usage along with other unique identification.

Importance of study / society application

- **International Status:**

Digital signing is universally accepted process in the various administrative procedures. The administrative reforms initiated in corporate sector are followed by various governments around the world. ICT has shown the impact to achieve better transparency, accuracy and speed. Along with the modern trends of web technology, the treats of security of sensitive data and restricting unauthorized user access are the challenges all over the globe.

Ease is the usage of DSC for various ICT applications is equally important to every part of the administrative process, irrespective of the national boundaries.

- **National Status:**

Year 2015 has emerged with dream of Digital India. It is the chief priority programme of Government of India with a vision to transform India into a digitally empowered society and knowledge economy. Most all of the Government process are reengineered and implication of ICT is has opened new era of G2C and G2G processes. The propagation of ICT has been reached to Districts and Block level. Most the citizen oriented government services has been given online through web based eGovernance applications. The Government of India and most of the states has established highly technical Data Centers. Use of ICT has become mandatory in the Government procedure.

The security of data is priority of technical drivers of these procedures. The authentic logins to the web servers for accessing data is prime responsibility of the developers. The use of DSC is binding to the government officials.

Significance of the study:

This research work is significant in many ways. It is important from the administrative point of view because it is focusing on the simplified usage of DSCs. This simplified usage will be extremely important as it directly simplifies the administrative procedure.

The present study is equally significant for the society because every eGovernance activity aims for facilitation of public. More over many citizens are also directly users of many eGovernance applications.

The present study is also significant for technical point of view. The outcome of this study will be significant input for the developers and coders as well as for the project managers of various eGovernance applications.

The present study is extremely important for the Government as well as citizens as it deals with current scenario of the Government procedures.

Proposed work plan

Month wise plan of work and targets to be achieved are as follows.

Time period	Planned work	Target to be acheived
0 to 12 Months	Study of CPS of various CAs in India.	Learning the methods of, • Certificate Application. • Certificate Issuance. • Certificate Download • Acceptance Certificate Revocation List (CRL) • System Security Audit Procedures
7 to 12 Months	Study of CPS of various CAs in India. (continued)	Learning methodology of, physical, procedural and personal security controls
12 to 24 Months	• Study of CPS of various CAs in India. (continued) • Discussios with technical staff of CAs if necessary.	Learning methods of, • Technical Security Controls. Key Pair Generation and Installation. • Private Key Protection. • Computer/Systems Security Controls. • Network Security Controls. • Cryptographic Module Engineering Controls
24 to 30 Months	Study of usage procedures	Confirmation of the Hypothesis
30 to 42 Months	Study of simplification in the process on the basis of unique identification.	• Suggestion of simplified usage procedure. • Verification of suggested algorithm against hypothesis.
42 to 48 Months	Documentation	Submission of Research Work

References

1. National Policy on Information Technology, 2012 (NPIT 2012) available at http://deity.gov.in/sites/upload_files/dit/files/National_20IT_20Policyt%20_20.pdf accessed 15th May 2016.
2. Strategies for E-Governance in India, available at, http://indiaegovernance.blogspot.in/2008/04/strategies-for-e-governance-in-india.html (blogpost by Shri. Abhijeet A. Joshi) accessed 15th May 2016.
3. Vision Areas of Digital India Program, available at http://negd.gov.in/, accessed 15th May 2016
4. "e-Governance : Initiatives in India", available at http://arc.gov.in, accessed 15th May 2016
5. "Vision & Mission", available at official website of DeiyT, http://deity.gov.in/, accessed 15th May 2016.
6. Services of NIC, available at http://www.nic.in/services accessed 15th May 2016.
7. THE INFORMATION TECHNOLOGY ACT, 2000, The Gazette of India, PART II (Section 1)
8. MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY (Department of Information Technology) S.O.1015(E)- In exercise of the powers conferred by sub-section (1) of section 86 of the Information Technology Act 2000 (21 of 2000)
9. INFORMATION TECHNOLOGY (CERTIFYING AUTHORITY) REGULATIONS, 2001 (Under Section 89 of the Information Technology Act, 2000) Issued by : Controller of Certifying Authorities (July 2001)
10. Certificate Practice Statement (CPS) Version1.0June04, 2015, OID:2.16.356.100.1.9.2, Published by CDAC.
11. Certificate Practice Statement (CPS) published by (n)Code Solutions CA, A DIVISION OF GUJARAT NARMADA VALLEY FERTILIZERS COMPANY LIMITED, Version 1.0
12. Certificate Practice Statement (CPS) published by Mudhra Limited, Version 2.2, Document Number eMCSL/e-Mudhra/DOC/CPS/2.2
13. Certificate Practice Statement (CPS) , **VERSION 3.2, published by IDRBT, Document No. IDRBTCA/DOC/CPS/3.2, July 2013**
14. Certificate Practice Statement (CPS) Version 1.2, published by Safecript Ltd.
15. Certificate Practice Statement (CPS) published by NICCA, Version 4.4, Document No. **OID: 2.16.356.100.1.4.2**
16. Certificate Practice Statement (CPS) published by TCS-CA TRUST NETWORK VERSION 1.1
17. Interoperability Guidelines for Digital Signature Certificates issued under Information Technology Act, Version 3.1, published by Controller of Certifying Authorities, Department of Information Technology, Ministry of Communications and Information Technology.
18. Jianglang Feng and Jindong Li, A New Certificate-based Digital Signature Scheme (2013) in Fourth International Conference on Emerging Intelligent Data and Web Technologies.
19. Lein Harn and Jian Ren, Generalized Digital Certificate for User Authentication and Key Establishment for Secure Communications (2011) in IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 10, NO. 7, JULY 2011.
20. Chen-huang WU, Self-Generated-Certificate Digital Signature (2010) in Fourth International Conference on Genetic and Evolutionary Computing

21. BAI Chen-Xi, Shi Rui, Shen Shi-Lei, He Xin, A New Digital Signature Scheme of ElGamal Type on Conic Curve over the Ring Zn (2010) in International Conference on Computer Application and System Modeling (ICCASM 2010)
22. Joon S. Park and Ravi Sandhu, Binding Identities and Attributes Using Digitally Signed Certificates (2000), 1063-9527/00 $10.00 0 2000 IEEE
23. Chris K. Williams, Science Applications International Corporation (SAIC), CONFIGURING ENTERPRISE PUBLIC KEY INFRASTRUCTURES TO PERMIT INTEGRATED DEPLOYMENT OF SIGNATURE,ENCRYPTION AND ACCESS CONTROL SYSTEMS.
24. Huaqun Wang, Shuping Zhao, Cryptanalysis and Improvement of Several Digital Signature Schemes (2010) in Second International Conference on Networks Security, Wireless Communications and Trusted Computing

***

Signature	Signature
Research Scholar	Research supervisor / Guide / Co-guide